

# Investor Presentation

November 2023



# Safe Harbor



*This presentation includes “forward-looking statements” within the meaning of the Private Securities Litigation Reform Act of 1995. Any statements made herein that are not statements of historical fact, including statements about Radware’s plans, outlook, beliefs or opinions, are forward-looking statements. Generally, forward-looking statements may be identified by words such as “believes,” “expects,” “anticipates,” “intends,” “estimates,” “plans,” and similar expressions or future or conditional verbs such as “will,” “should,” “would,” “may” and “could.” Because such statements deal with future events, they are subject to various risks and uncertainties, and actual results, expressed or implied by such forward-looking statements, could differ materially from Radware’s current forecasts and estimates. Factors that could cause or contribute to such differences include, but are not limited to: the impact of global economic conditions and volatility of the market for our products; the effects of the current attacks by the terrorist groups Hamas and Hezbollah, and the war between Israel and Hamas and Israel and Hezbollah; natural disasters and public health crises, such as the COVID-19 pandemic; A shortage of components or manufacturing capacity could cause a delay in our ability to fulfill orders or increase our manufacturing costs; Our business may be affected by sanctions, export controls and similar measures targeting Russia and other countries and territories as well as other responses to Russia’s military conflict in Ukraine, including indefinite suspension of operations in Russia and dealings with Russian entities by many multi-national businesses across a variety of industries; our ability to expand our operations effectively; timely availability and customer acceptance of our new and existing solutions; risks and uncertainties relating to acquisitions or other investments; the impact of economic and political uncertainties and weaknesses in various regions of the world, including the commencement or escalation of hostilities or acts of terrorism; intense competition in the market for cyber security and application delivery solutions and in our industry in general and changes in the competitive landscape; changes in government regulation; outages, interruptions or delays in hosting services or our internal network system; compliance with open source and third-party licenses; the risk that our intangible assets or goodwill may become impaired; our dependence on independent distributors to sell our products; long sales cycles for our solutions; changes in foreign currency exchange rates; real or perceived shortcomings, defects or vulnerabilities in our solutions or if we or our end-users experience security breaches; the availability of components and manufacturing capacity; our reliance on a single managed security service provider to provide us with scrubbing center services; the ability of vendors to provide our hardware platforms and components for our main accessories; our ability to protect our proprietary technology; intellectual property infringement claims made by third parties; changes in tax laws; our ability to realize our investment objectives for our cash and liquid investments; our ability to attract, train and retain highly qualified personnel; and other factors and risks over which we may have little or no control. This list is intended to identify only certain of the principal factors that could cause actual results to differ. For a more detailed description of the risks and uncertainties affecting Radware, refer to Radware’s Annual Report on Form 20-F, filed with the Securities and Exchange Commission (SEC) and the other risk factors discussed from time to time by Radware in reports filed with, or furnished to, the SEC. Forward-looking statements speak only as of the date on which they are made and, except as required by applicable law, Radware undertakes no commitment to revise or update any forward-looking statement in order to reflect events or circumstances after the date any such statement is made. Radware’s public filings are available from the SEC’s website at [www.sec.gov](http://www.sec.gov) or may be obtained on Radware’s website at [www.radware.com](http://www.radware.com).*

# Radware Complete Mitigation Suite

## Radware's Core Business

### Application Availability

Application delivery



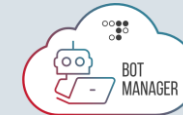
### Application and Data Center Security

Mitigation of denial-of-service and application attacks



### Cloud Security As-a-Service

Mitigation of data centers, web applications, API and automated attacks



## The Hawks Business

### SkyHawk

Protection of application hosted in the public cloud



### EdgeHawk

Protection of carriers' Edge

# Why Radware?



Leading Critical Cyber Security Vendor



Large Growing TAM and SAM



Leading Differentiated Technology



Large Enterprise and Carriers Customer Base



Fast Growing Cloud Security Business



Sustainable Growth and Profitability

# Industry Trends

Leading Critical Cyber Security Vendor



Growing  
Threat  
Landscape

Cloud  
Transition

Accelerated  
Digital  
Transformation

Shortage  
in Security  
Experts &  
Skills

# Industry Trends

Leading Critical Cyber Security Vendor



Growing  
Threat  
Landscape

Critical, Need  
State-of-the-Art  
Security

Cloud  
Transition

Accelerated  
Digital  
Transformation

Shortage  
in Security  
Experts &  
Skills

# Growing Threat Landscape



Shift in  
Attackers'  
Motivation

Shift to  
Attacks on  
Application  
Layer (incl.  
Web DDoS)

Shift to  
Automated  
Tools

# Attach Campaign On Health Care February 2023



TOPICS INDUSTRY EVENTS PODCASTS RESEARCH RECOGNITION

Threat intelligence, Application security, Vulnerability management



## Killnet DDoS attacks inflicting damage on healthcare: 'This is war'

Jessica Davis February 13, 2023



Recent alerts to the health sector warn that the Russia-Ukraine war have spurred hacktivists to leverage more destructive tactics. (iStock via Getty Images)

The Killnet hacktivist group's DDoS attacks against healthcare and the mass data exfiltration in January was reportedly just the first round of targeting. Industry leaders have grown increasingly concerned over the impact of nation-state actors and the

<https://www.scmagazine.com/news/threat-intelligence/killnet-ddos-attacks-inflicting-damage-on-healthcare-this-is-war>



Personal Business Pricing Partners

Search Labs



CYBERCRIME | NEWS

## KillNet hits healthcare sector with DDoS attacks

Posted: February 10, 2023 by Pieter Arntz

At the end of January, the Health Sector Cybersecurity Coordination Center warned that the KillNet group is actively targeting the US healthcare sector with distributed denial-of-service (DDoS) attacks.

The Cybersecurity and Infrastructure Security Agency (CISA) says it helped dozens of hospitals

<https://www.malwarebytes.com/blog/news/2023/02/killnet-group-targets-us-and-european-hospitals-with-ddos-attacks>

← Automatic Translation  
Russian → English

🔴 ATTENTION TO TEAMS THAT JOIN OUR MISSION!

👉 Everyone hit L7 on 50 hospital targets - 50 states of America!

Alaska  
<https://www.providence.org>  
<https://check-host.net/check-report/e77f515k82d>

Arizona  
<https://www.abrazohealth.com>  
<https://check-host.net/check-report/e77f5a2kcbce>

Arkansas  
<https://arksurgicalhospital.com>  
<https://check-host.net/check-report/e779e33kf96>

California  
<https://www.sclhealth.org>  
<https://check-host.net/check-report/e7821b1kf6>

Colorado  
<https://www.sclhealth.org>  
<https://check-host.net/check-report/e7821b1kf6>

Connecticut  
<https://gfp.griffinhealth.org>  
<https://check-host.net/check-report/e781374kbab>

Delaware  
<https://christianacare.org>  
<https://check-host.net/check-report/e77a063kb3e>

Florida  
<https://www.leehealth.org>  
<https://check-host.net/check-report/e77fbeck78c>

Georgia  
<https://www.northside.com>  
<https://check-host.net/check-report>



# Claimed Attacks on Telegram: Global

## Canadian PM (June 2023)



Узнали, что канадский премьер Джастин БибберТрюдо приперся на Украину подлизывать бандеровцам 🤡

Приложили за это его официальный сайт:

✗ <https://check-host.net/check-report/1034a6dckd6c>

Делаем это примерно в 100500-й раз 🤡

- 👉 Подписывайтесь на канал NoName057(16)
- 👉 Вступайте в наш DDoS-проект
- 👉 Подписывайтесь на резервный канал
- 👇 Eng version

🇺🇸 Победа За нами!

[t.me/noname05716/3634](https://t.me/noname05716/3634)

5.0K 👁 edited Jun 10 at 13:35

## UPS (April, June & Sept. 2023)



Anonymous Sudan

ut Anonymous Sudan

• <https://www.ups.com/> | United Parcel Service is an ...

وقفنا الهجوم على UPS ، وحنكتفي بال "ساعتين".

The attacks on the UPS have been stopped, we will be satisfied with this amount of "2 hours".

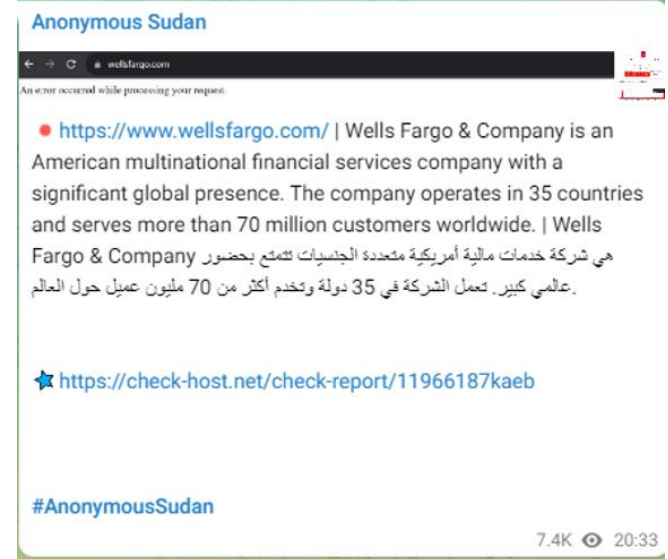
🔥 32 🤡 3 🦊 3 🌑 1 😂 1 😊 1

👁 19.3K edited 19:56

UPS outages reported in the last 24 hours



## Wells Fargo (Sept. 2023)



Anonymous Sudan

ut Anonymous Sudan

• <https://www.wellsfargo.com/> | Wells Fargo & Company...



Online Banking is temporarily unavailable

You can still access your accounts through our ATMs, banking locations, and customer service. Our phone bankers are available 24 hours a day, 7 days a week. We accept all relay calls, including 711.

6.6K 👁 20:35

# #OpIsrael 2023: Anonymous Sudan Joins the Islamic Jihad

Launches cyber attacks against Israeli sites (gov't, utilities, energy, civil defense)



Israeli Early Warning App (Red Colour)

نحن الآن نهاجم صهارات الإنذار في إسرائيل ، بما في ذلك القبة الحديدية " بالتوفيق يا غزة " " Good luck Gaza "

We are now attacking the sirens in Israel, including Iron Dome

Anonymous Sudan

Connection timed out

Bad gateway

What happened? The web server reported a bad gateway error.

What can I do? Please try again in a few minutes.

Latest Real Time Signature

- Number of Path Elements = 0 AND
- HTTP Method = GET AND
- Number of Query Arguments = 0, 1 AND
- Number of Cookies = 0 AND
- Number of Standard Headers = 3, 4, 5 AND
- Header 'cache\*' does not exist AND
- Header 'if-\*' does not exist AND
- Header 'referer' does not exist AND
- Header 'sec-\*' does not exist AND

Sept'23: Attack blocked by Radware

Israeli News Portal: Rotter.net

بشكل كامل "خارج الخدمة"

[rotter.net](http://rotter.net)

Completely "out of service"

#AnonymousSudan

Telegram

Anonymous Sudan

For inquiries: [https://t.me/AnonymousSudan\\_Bot](https://t.me/AnonymousSudan_Bot)

Chat: <https://t.me/AnonymousSudanChat>

Bad gateway

What happened? The web server reported a bad gateway error.

What can I do? Please try again in a few minutes.

May'23: Attack bypassed Cloudflare; site went down

# New Disruptive Web DDoS Tsunami Attacks

Requires a  
behavioral-based  
approach for  
accurate detection &  
mitigation



Higher in volume – Ultra high RPS



Encrypted floods



Appear to be legitimate requests



Multiple, sophisticated evasion techniques  
(randomized headers, IP spoofing, etc)

# Standard Protections are Not Effective

Network-Based DDoS protection cannot detect & mitigate L7 DDoS attacks

Standard WAF solutions look for vulnerability exploits

Rate-limiting techniques impact legit traffic



Available mitigation tools ineffective in detecting & mitigating HTTP/S floods **without impacting legitimate web traffic!**

# Industry Trends

Leading Critical Cyber Security Vendor



Growing  
Threat  
Landscape

Critical, Need  
State-of-the-Art  
Security

Cloud  
Transition

Consistent  
Security  
Across Clouds

Accelerated  
Digital  
Transformation

Shortage  
in Security  
Experts &  
Skills

# Cloud Transition Introduces Uncertainties

Pace & Final Deployment Unknown

## Multi-Cloud Creates New Security Risks



**99%** Deploy Applications in at Least One Public Cloud

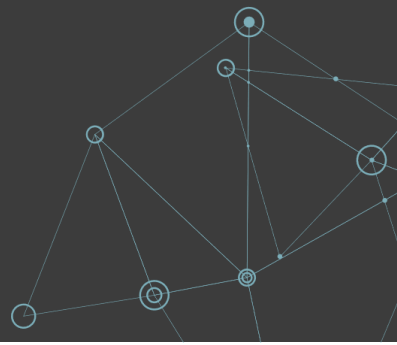
**69%** Experienced Data Exposure Due to Inconsistencies Between Platforms

**70%** Aren't Confident in Level of Security by Their Public Cloud Vendor

Need for **consistent security** across all clouds

# Industry Trends

Leading Critical Cyber Security Vendor



Growing  
Threat  
Landscape

Critical, Need  
State-of-the-Art  
Security

Cloud  
Transition

Consistent  
Security  
Across Clouds

Accelerated  
Digital  
Transformation

Frictionless  
Security

Shortage  
in Security  
Experts &  
Skills

# Accelerated Digital Transformation



Multiple End-Users & Partners



Distributed Workforce



Increased Use of APIs



Online Consumption of Goods



Applications  
at Center  
of Business



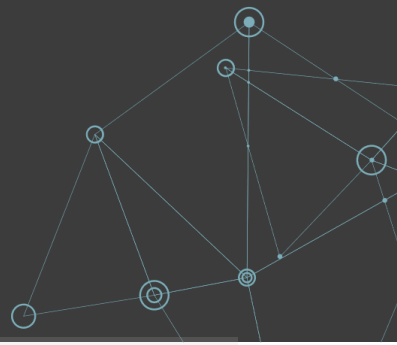
**Time to market** and **agility**  
are critical to staying  
competitive

Need **frictionless security** that does not hold you back



# Industry Trends

Leading Critical Cyber Security Vendor



Growing  
Threat  
Landscape

Critical, Need  
State-of-the-Art  
Security

Cloud  
Transition

Consistent  
Security  
Across Clouds

Accelerated  
Digital  
Transformation

Frictionless  
Security

Shortage  
in Security  
Experts &  
Skills

Automated  
Protection and Fully  
Managed Services

# Shortage in Security Experts & Skills

+25%

demand for  
cyber security  
experts

~3.4M

open positions  
worldwide

70%

businesses are  
facing skill  
shortages

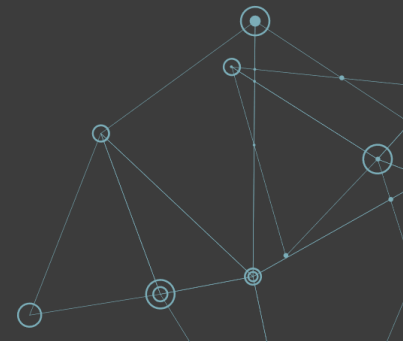
43%

can't find enough  
qualified talent

Need for **automated protections** and **fully managed services**

# Industry Trends

Leading Critical Cyber Security Vendor



Growing  
Threat  
Landscape

Critical, Need  
State-of-the-Art  
Security

Cloud  
Transition

Consistent  
Security  
Across Clouds

Accelerated  
Digital  
Transformation

Frictionless  
Security

Shortage  
in Security  
Experts &  
Skills

Automation  
Fully Managed

# What is Needed to Stay Ahead?



## REAL-TIME

Immediate, real-time protection from advanced, unknown threats

## INTELLIGENT

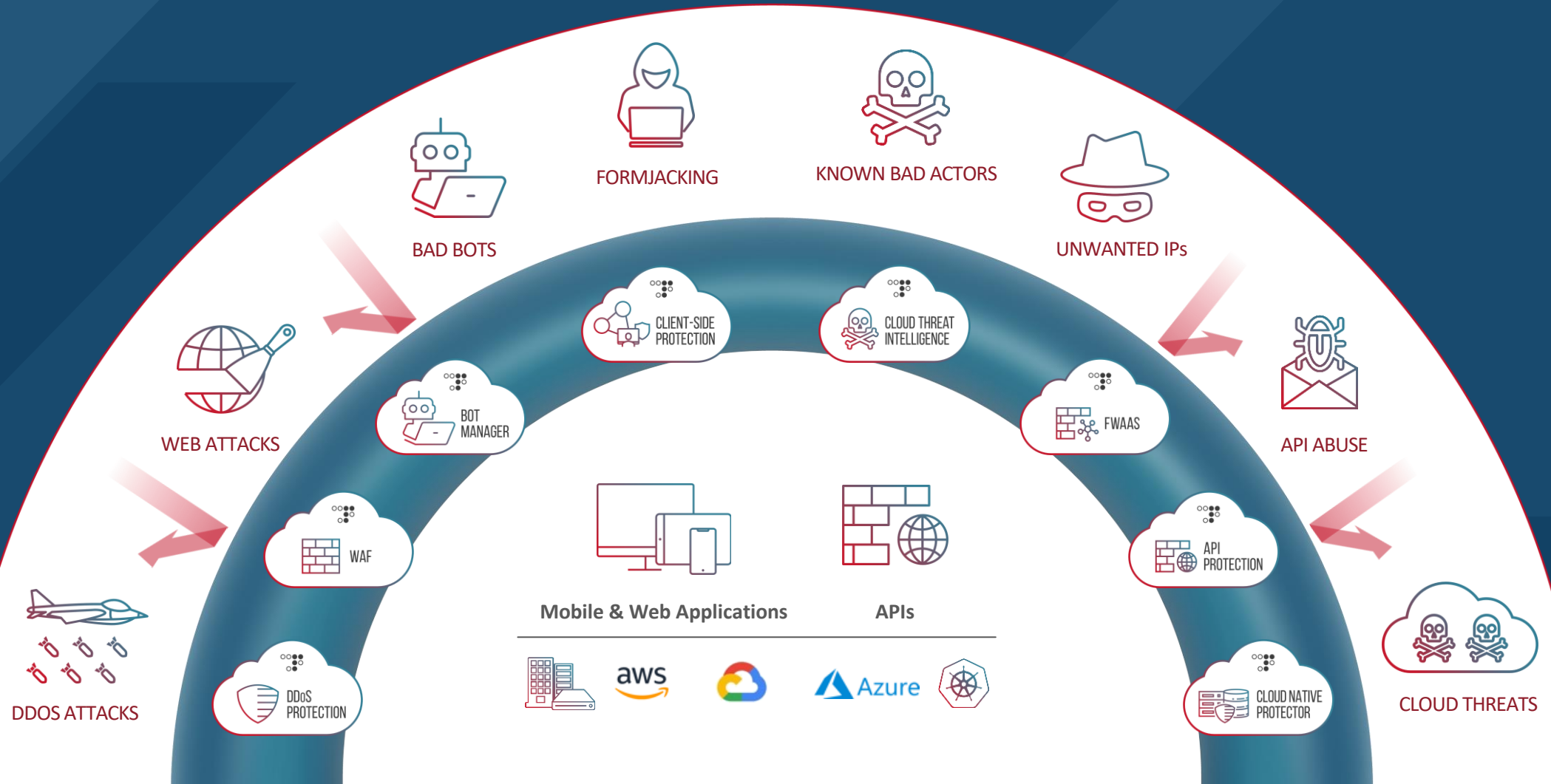
Automated protections based on AI + ML-based algorithms that evolve as the attacks morph

## UNIVERSAL

360-degree, consistent protection across all environments and entry points

# Radware 360 Application Protection

Dedicated to Your Application Protection. Real-Time, Intelligent & Universal.



# The Radware Difference

Dedicated to Your Application Protection. Real-Time, Intelligent & Universal.



## REAL-TIME

- Immediate Protection
- Behavioral-based Zero-Day Attack Protection
- Advanced challenges (crypto challenge)



## INTELLIGENT

- AI & ML Algorithms
- Adaptive & Continuous Learning
- Auto Detection & Mitigation
- No Human Intervention Required



## UNIVERSAL

- Agnostic, Consistent & Integrated
- Across All Environments, K8S, APIs & Browser-side
- Expert & Managed Services

# State-of-the-Art Protection: Winning Industry Recognition

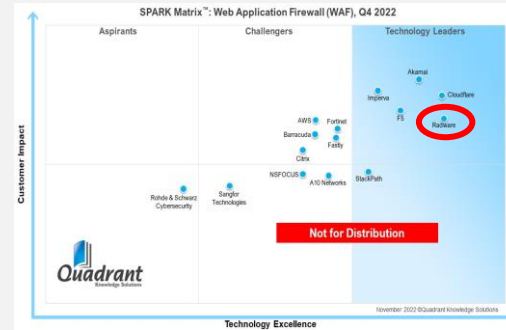
## BOT MANAGEMENT 2023 LEADER



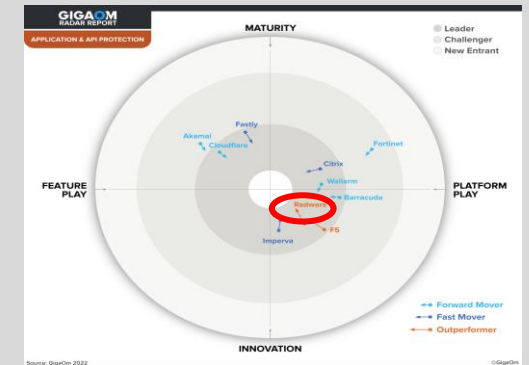
## DDoS 2023 LEADER



## WAF 2023 LEADER



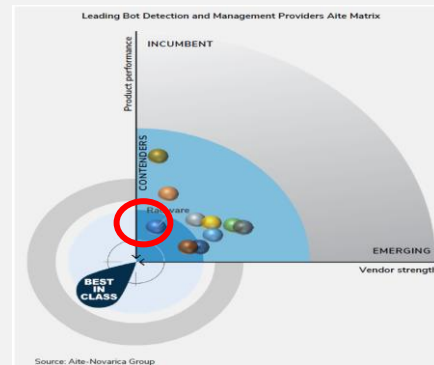
## APP & API PROTECTION 2022 LEADER & OUTPERFORMER



## BOT DETECTION MATRIX, 2022 BEST IN CLASS



*“The largest global financial institutions, brokerage firms, and financial services companies use Radware’s Bot Manager.”*



## WAF LEADERSHIP COMPASS 2022 OVERALL LEADER Product, Innovation & Market Leader



# State-of-the-Art Protection: Winning Industry Recognition

Gartner.  
Peer Insights™

98%

WOULD RECOMMEND  
Radware Cloud WAF  
Service

94%

WOULD RECOMMEND  
Radware Cloud DDoS  
Protection Service

## Radware Cloud DDoS Protection Service Reviews

by Radware in DDoS Mitigation Services  
4.8 ★★★★★ 19 Ratings

## Radware DefensePro Reviews

by Radware in DDoS Mitigation Services  
4.9 ★★★★★ 25 Ratings

## Radware Cloud WAF service Reviews

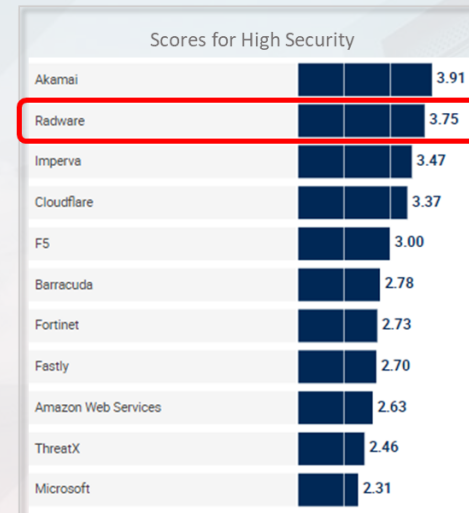
by Radware in Cloud Web Application and API Protection  
4.7 ★★★★★ 124 Ratings

\* Gartner Peer Insight as of Feb. 20<sup>th</sup> 2023

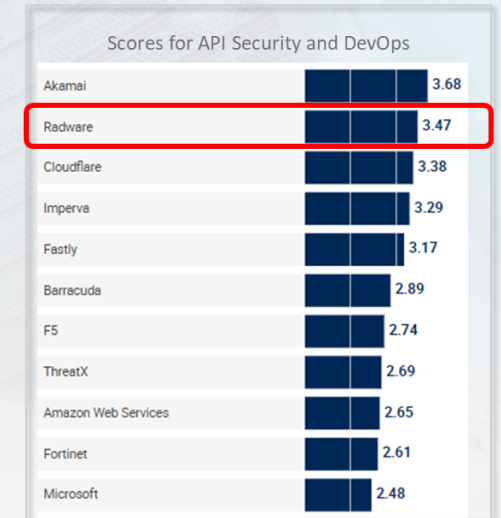
Gartner

CRITICAL CAPABILITIES FOR CLOUD WEB APPLICATION  
AND API PROTECTION (WAAP), 2022

#2 IN HIGH SECURITY & API USE CASES



*“Radware Cloud WAF  
Service is a **good**  
candidate, especially for  
the high-security use case”*

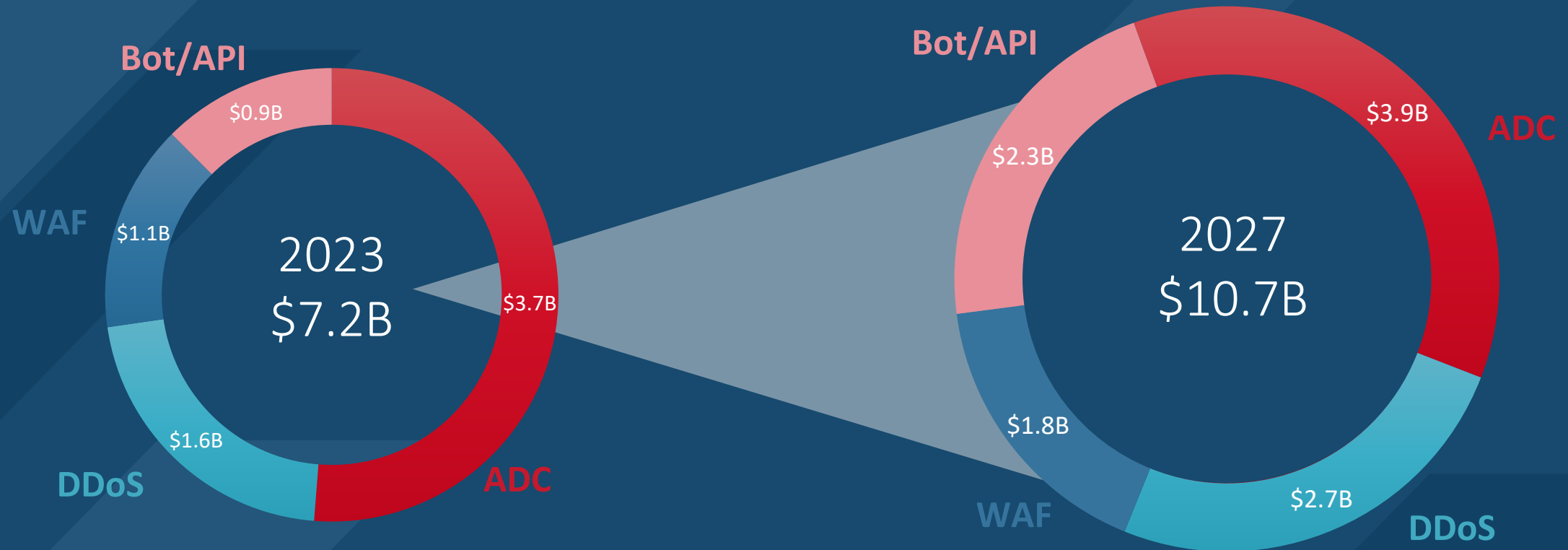


*“Radware offers one of the  
stronger API security  
offerings on the WAAP  
market”*



# Growth Strategy: Profitable Growth Powered by Cloud Security

# The Markets We Operate In



Source: IDC: Worldwide Application Protection and Availability Forecast, 2022–2026: Security Powers the Digital Experience, November 2022

# Large Enterprise and Service Providers

## Blue Chip Customers



6 OF TOP 10

WORLD'S  
BANKS



7 OF TOP 10

WORLD TELECOM  
COMPANIES



6 OF TOP 12

WORLD'S STOCK  
EXCHANGES



4 OF TOP 10

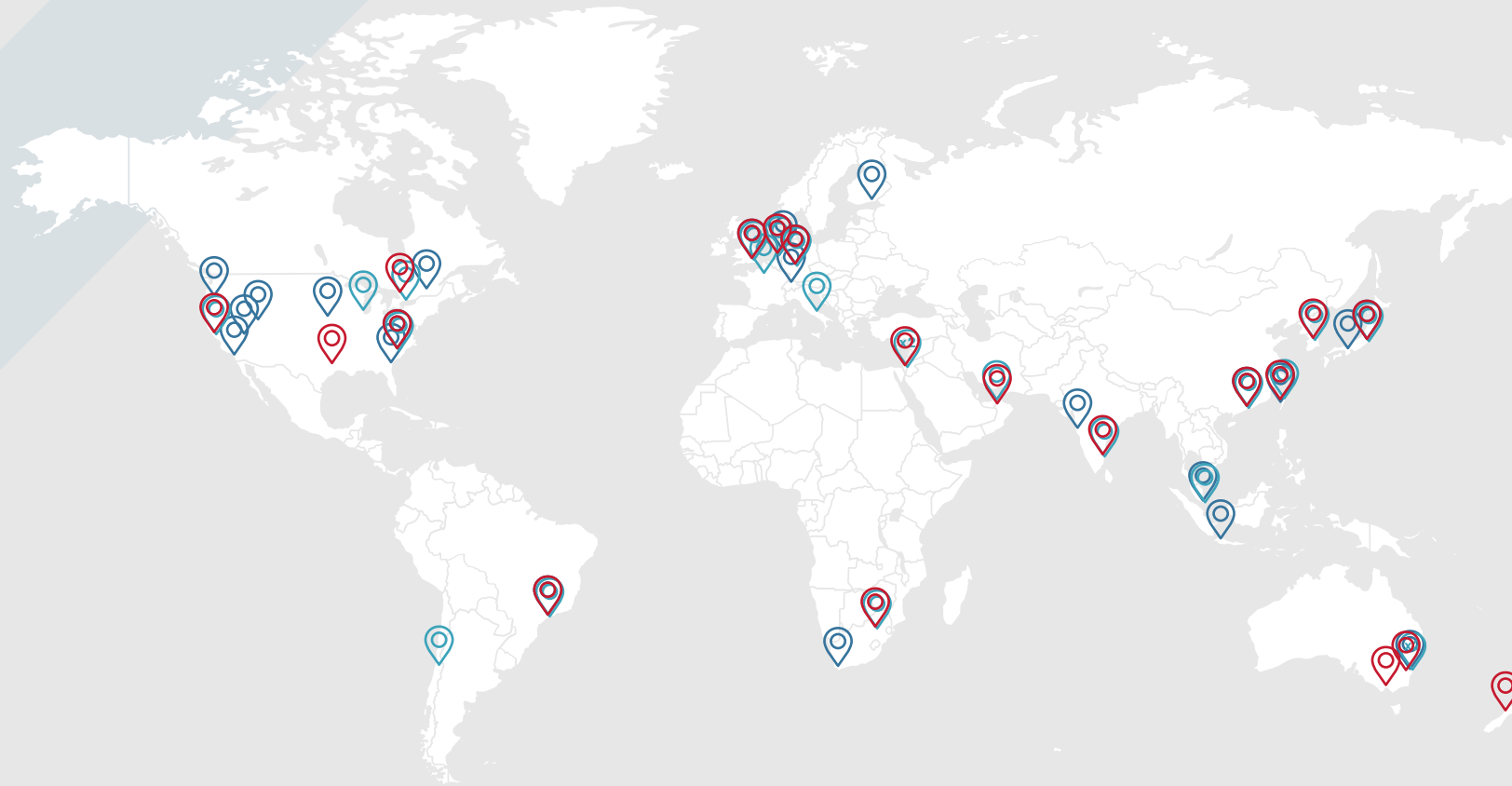
WORLD'S  
ECOMMERCE  
COMPANIES



4 OF TOP 10

MOST WIDELY  
USED SAAS  
APPLICATIONS

# Global Cloud Services Network



19 SCRUBBING CENTERS  
Worldwide

12 Tbps OF GLOBAL  
MITIGATION CAPACITY

40+ AppSec  
PoPs

WITH GLOBAL COVERAGE



DDoS MITIGATION SCRUBBING CENTER



CLOUD WAF PoP




BOT MANAGER SERVICE CENTER

# Radware Strategy Summary



- 1** On-Prem Business  
TAM is growing, best of breed required
- 2** Critical Areas  
Large, strong and profitable
- 3** Accelerating Cloud Security Business  
Strong growth, expanding SAM, SaaS business model
- 4** Leverage in the Model  
Driving profitable growth with OpEx leverage

# Environment, Social, Governance



## Establishing a Clean, Ethical and Human Future



### Protecting the Environment

- Implemented KPIs for reduction in the use of water, power and paper
- Providing energy saving products to our customers
- Setting environmental policy goals in measuring impact, consideration in operation and informing proper use of our products



### Promoting Human Rights

- Published Human Rights and Labor Standard Policy
- Radware was named in the Top 100 Workplaces for Diverse Representation by Mogul
- Encourage a culture of open dialogue and support and attend to our employees' wellbeing



### Investing in Community

- Building strong relationship with the community with various projects
- Empowering next-cyber generation with interns and mentoring high school students
- Empowering women through education or supporting business
- Promoting inclusion of underrepresented communities

# Financial Overview



# Q3 2023 Highlights

\$62M

## Revenue

13% decrease  
YoY

79%

## Recurring Revenue

Compared to  
71% last year

81.1%

## Gross Margin

Compared to  
82.9% last  
year

\$204M

## Total ARR

5% increase  
YoY\*

\$63M

## Cloud ARR

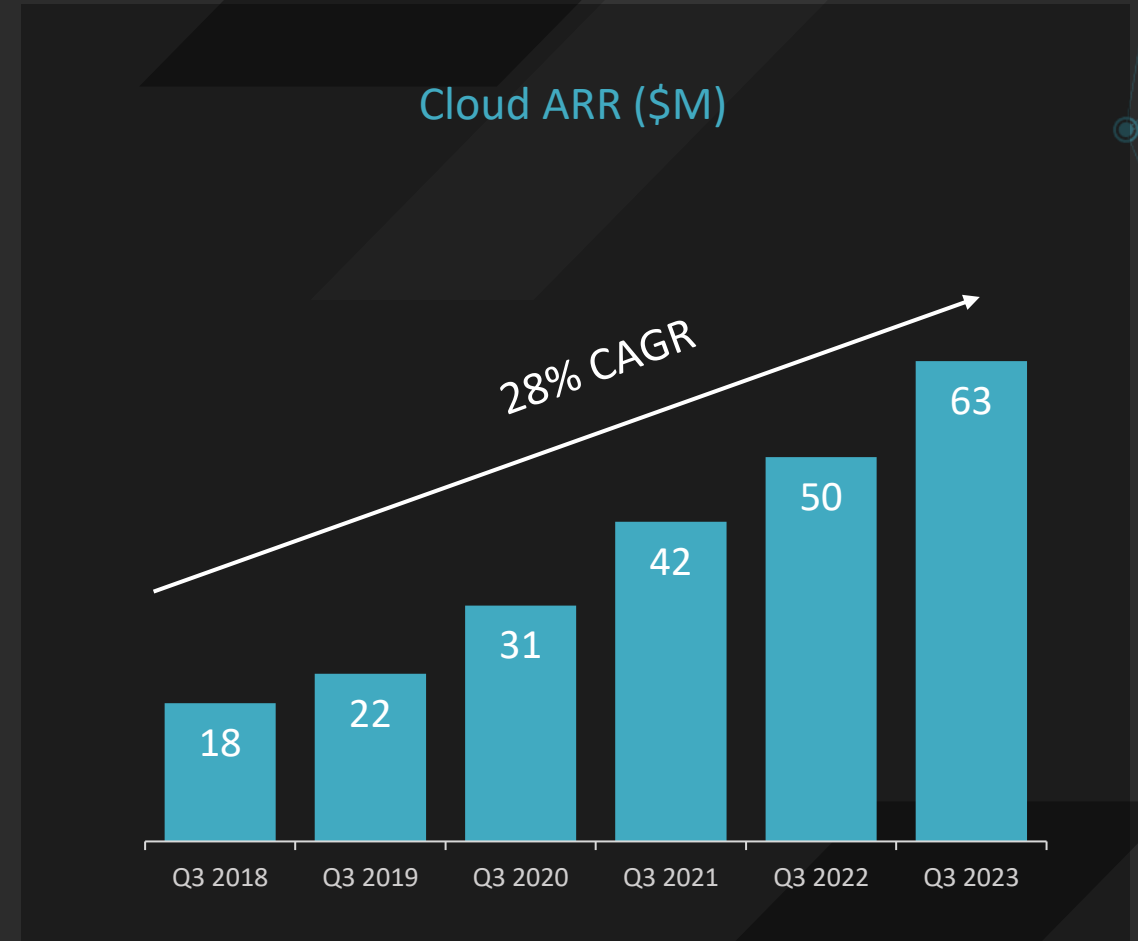
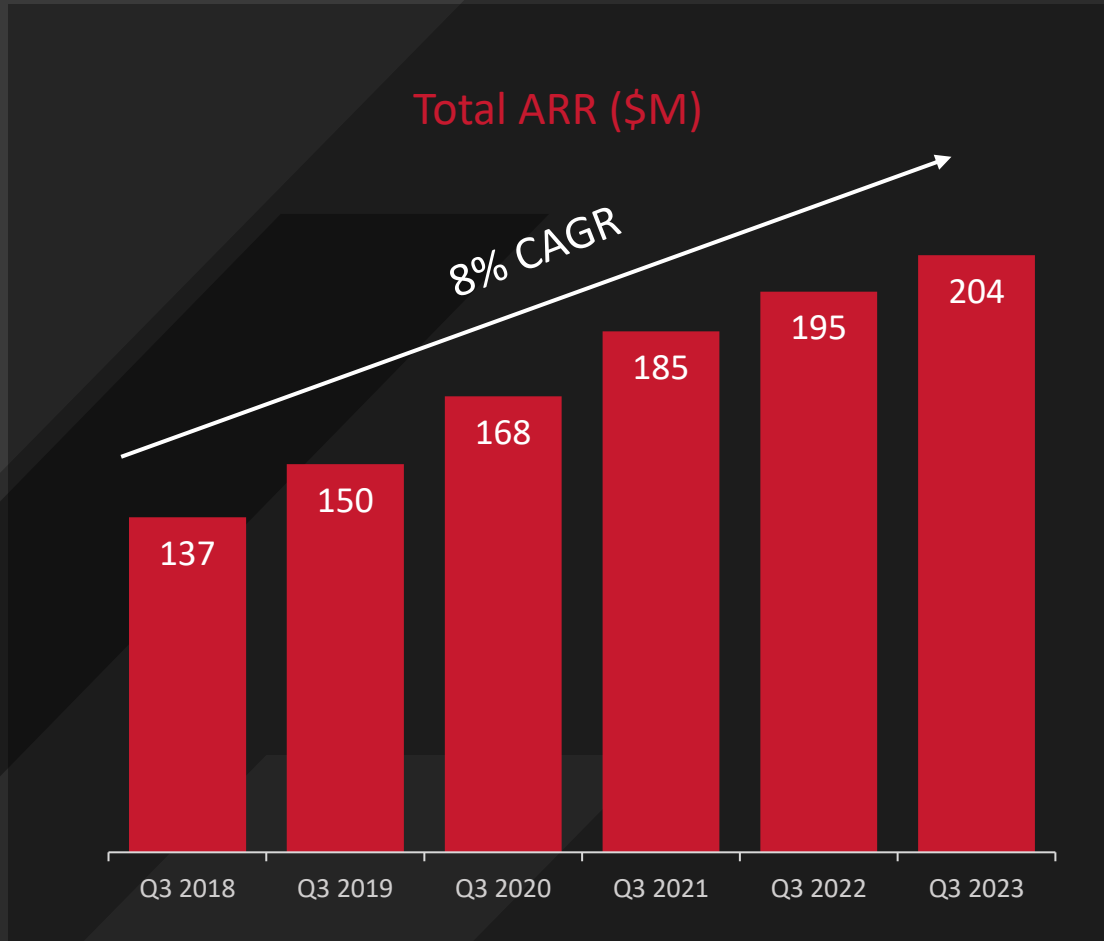
25% increase  
YoY

*\* Total ARR includes the annualized value of booked orders for services, subscription licenses and maintenance contracts that are in effect at the end of a reporting period*

*\* Total ARR growth of 8% when excluding ARR churn from previous quarters due to the unique customer relationship*



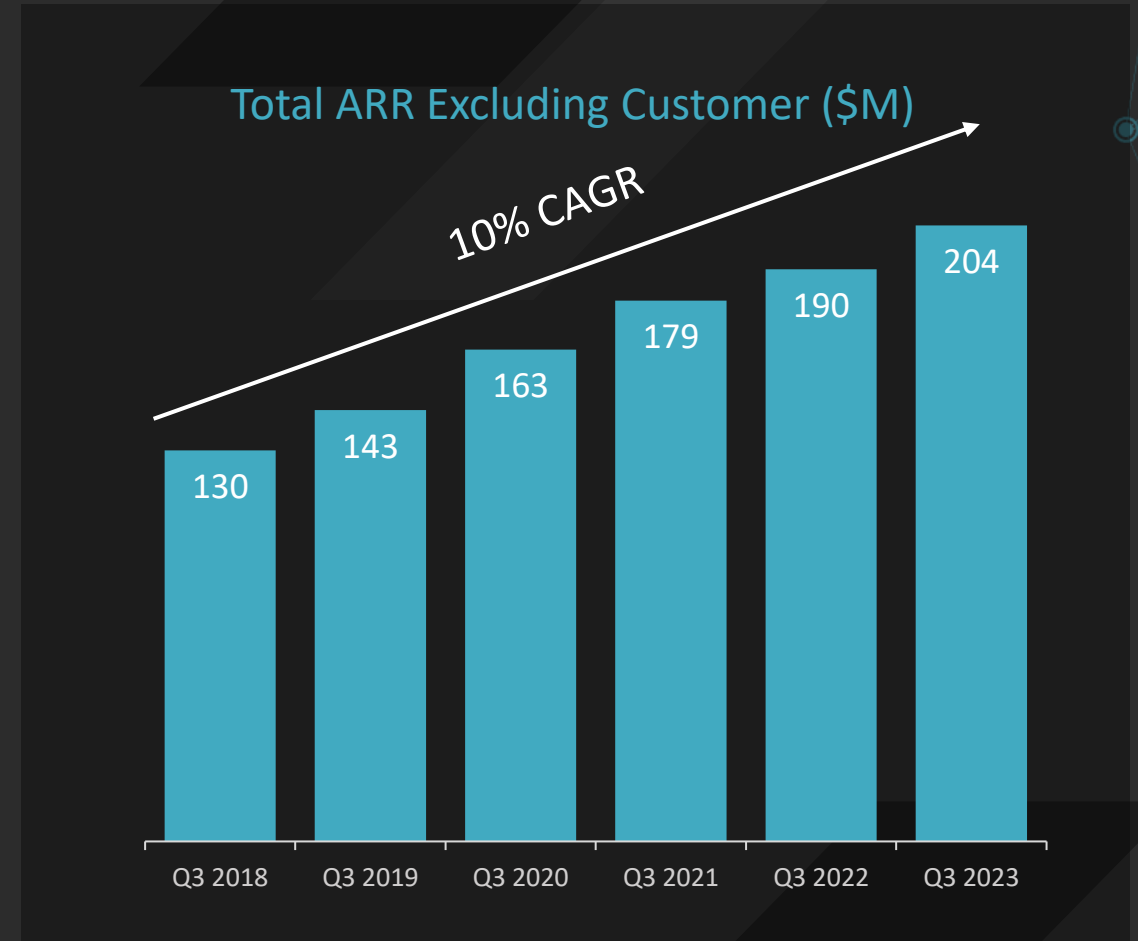
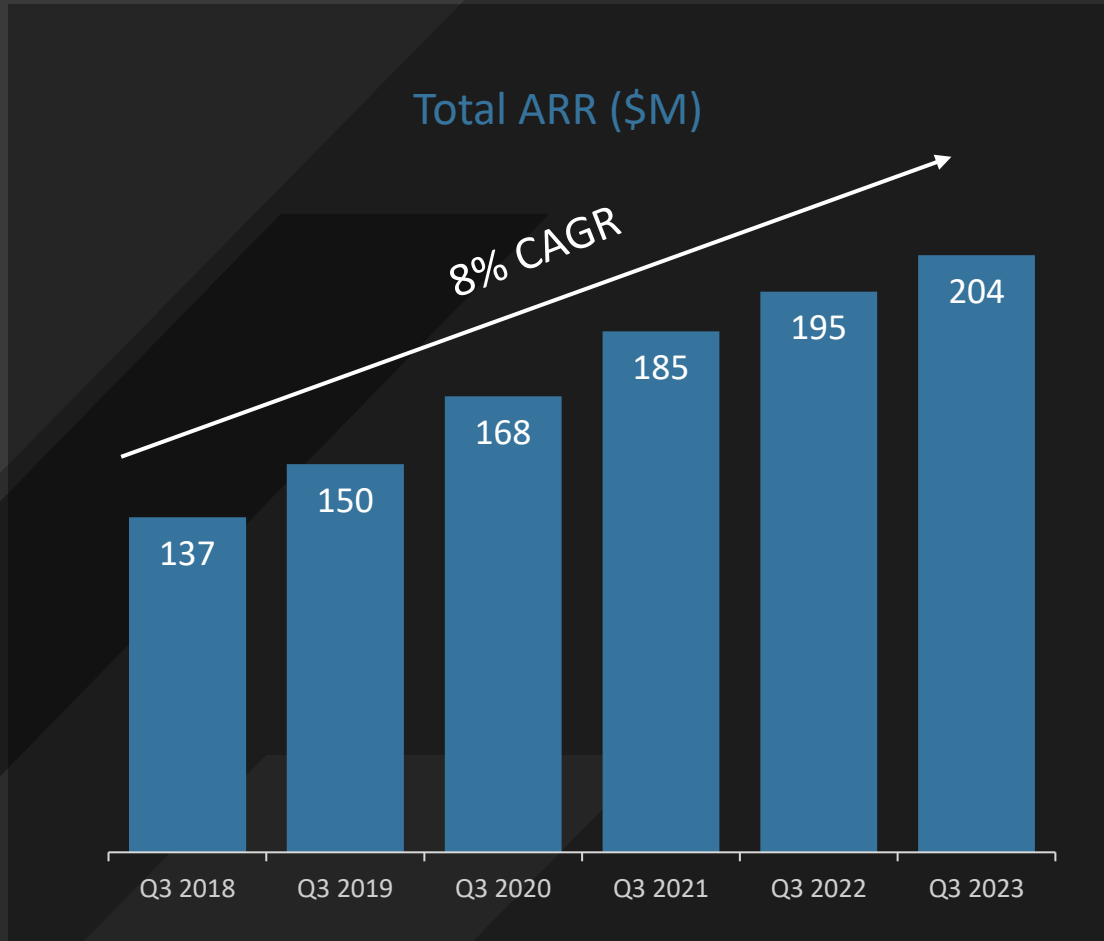
# ARR Driven by Cloud ARR (\$M)



\* Total ARR includes the annualized value of booked orders for services, subscription licenses and maintenance contracts that are in effect at the end of a reporting period

\* ARR numbers are rounded

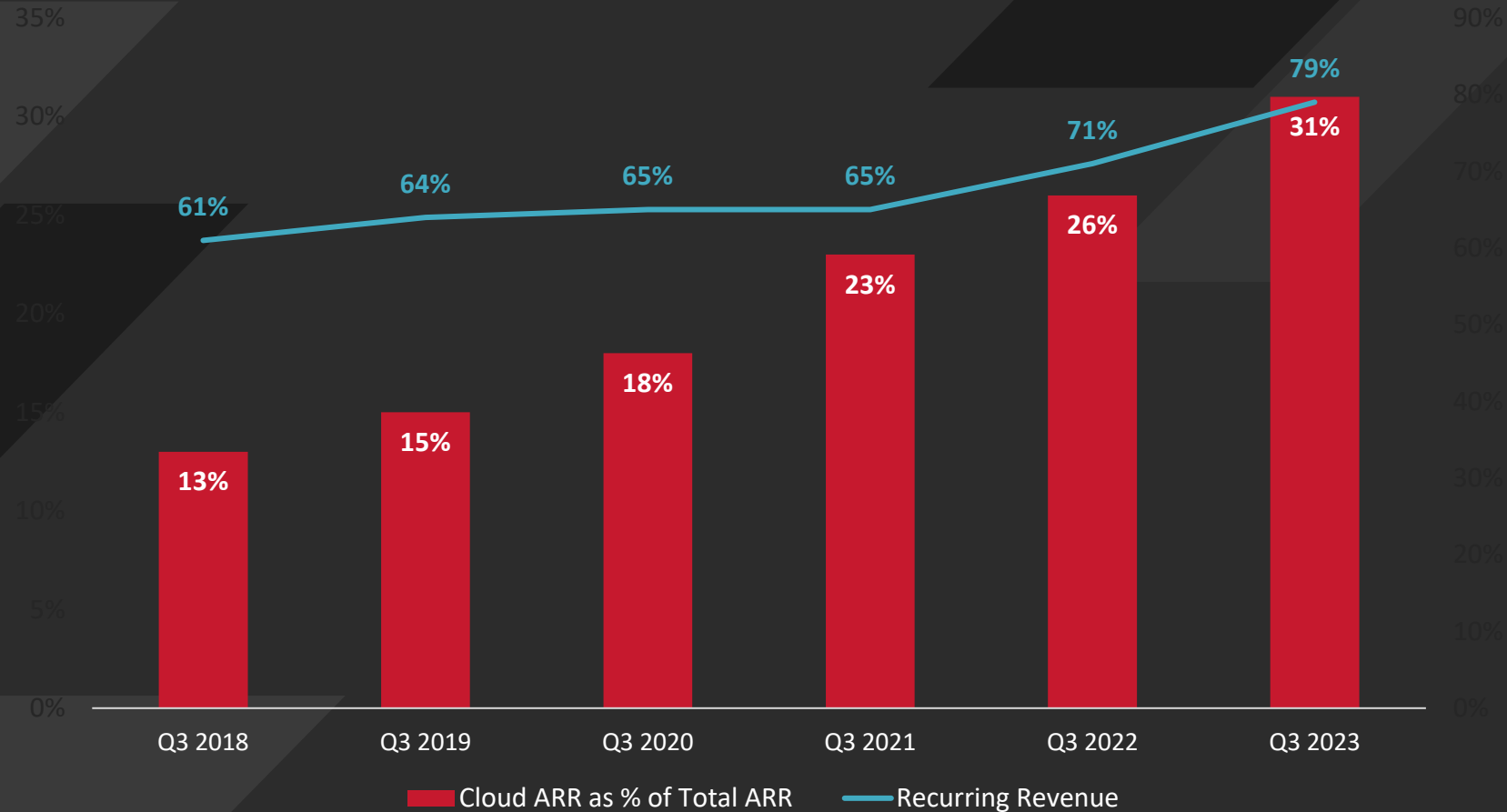
# Total ARR Excluding Customer Termination Agreement



\* Total ARR includes the annualized value of booked orders for services, subscription licenses and maintenance contracts that are in effect at the end of a reporting period

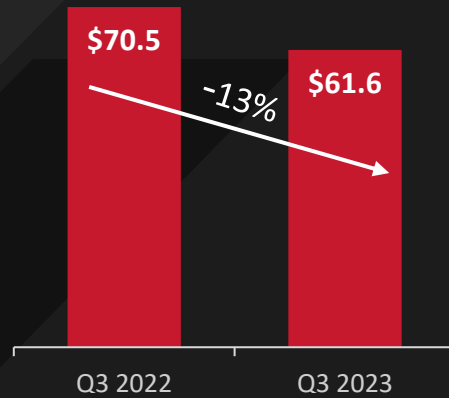
\* ARR numbers are rounded

# Recurring Revenue (%) Driven by Cloud ARR (\$M)

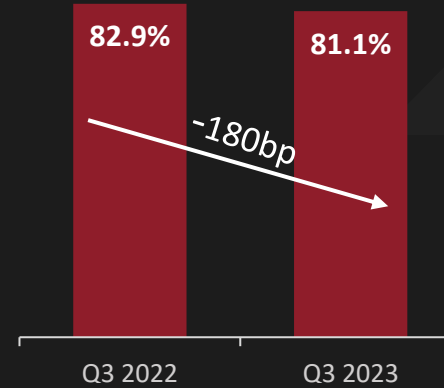


# Non-GAAP Financial Data

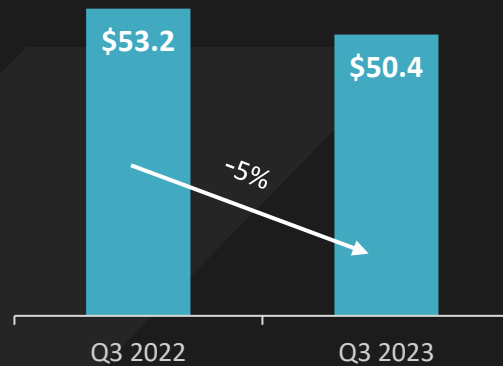
## Total Revenue (\$M)



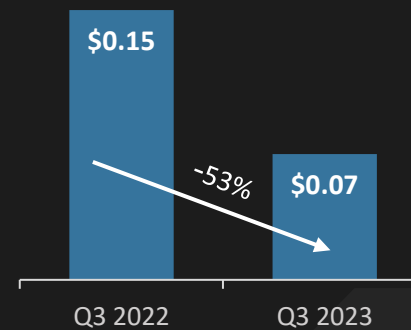
## Gross Margin



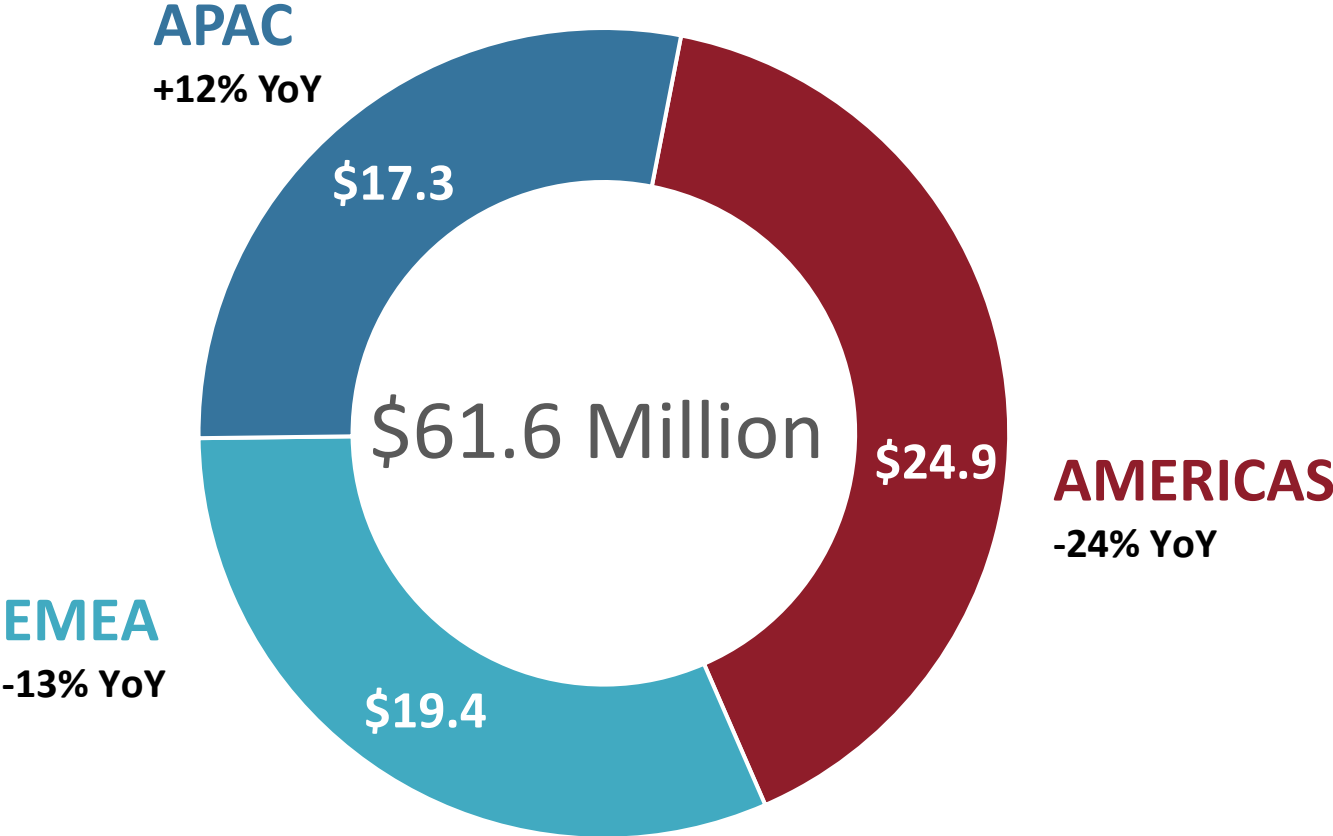
## Operating Expenses (\$M)



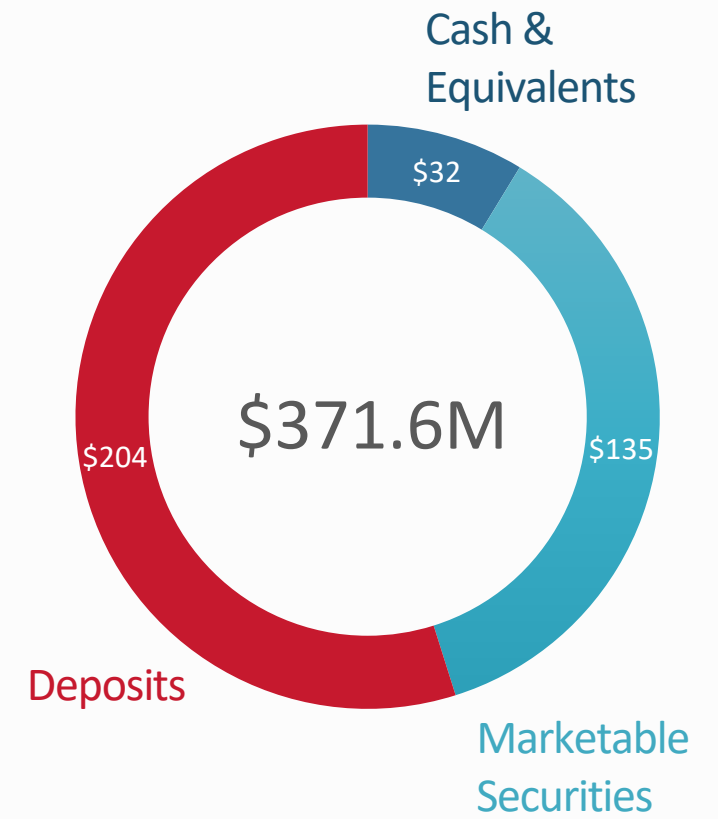
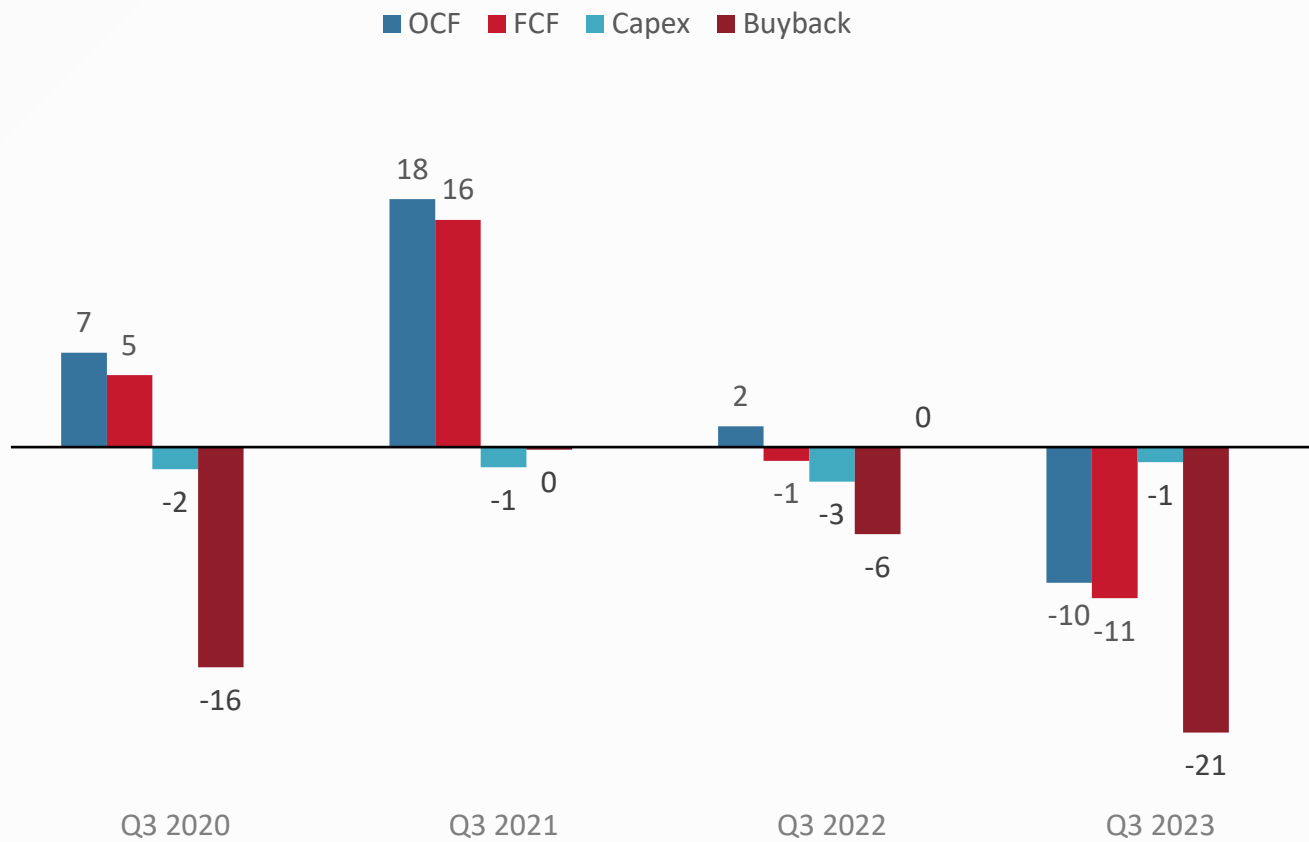
## EPS (\$)



# Q3 2023 Revenue Breakdown by Geographies (\$M)



# Cash Generation



# Thank You!

